Akraino Platform Security Architecture Whitepaper

March 2023

Daniil Egranov, Arm

Purpose and Target Audience

- **Define core security requirements for Akraino platforms and blueprint execution environments.**
- **Provide a mechanism for defining platform security requirements to blueprint owners.**
- **Provide security guidance to blueprint integrators.**

- **Whitepaper targets the following audience:**
  - **Akraino Blueprint owners and developers**
  - **Akraino platform owners**
  - **Cloud environment providers**
  - **Akraino Blueprint integrators**

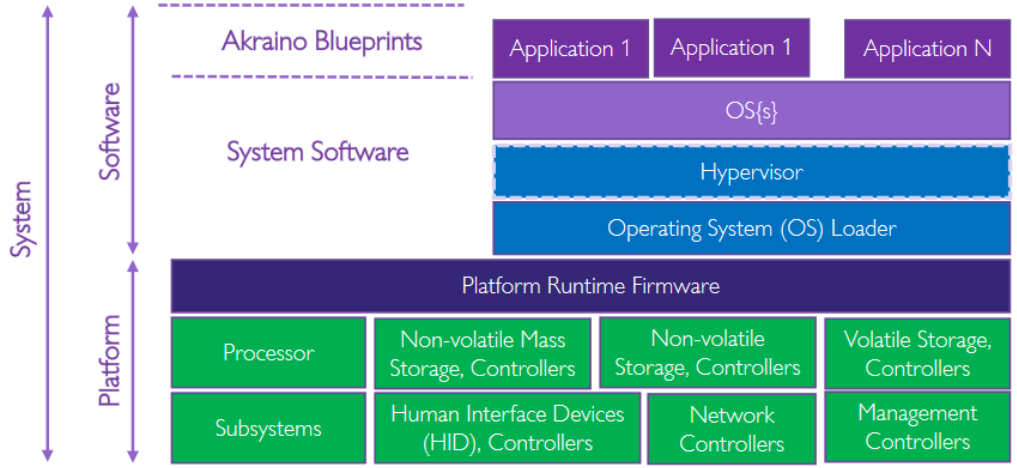
AKRAINO

Goals and Objectives

The goal of platform security is to secure all layers and components within a platform. This enables securing an entire platform by using unified security requirements.

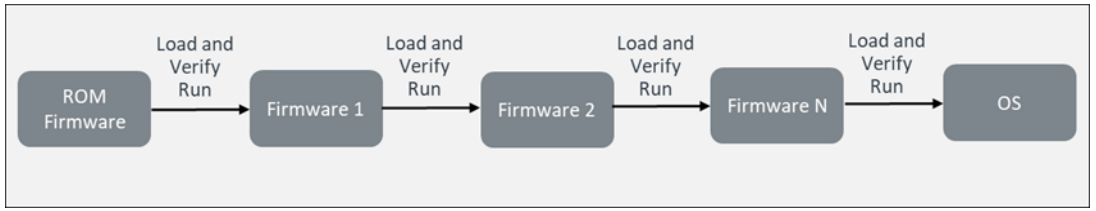
The core objectives of platform security for the Akraino project:

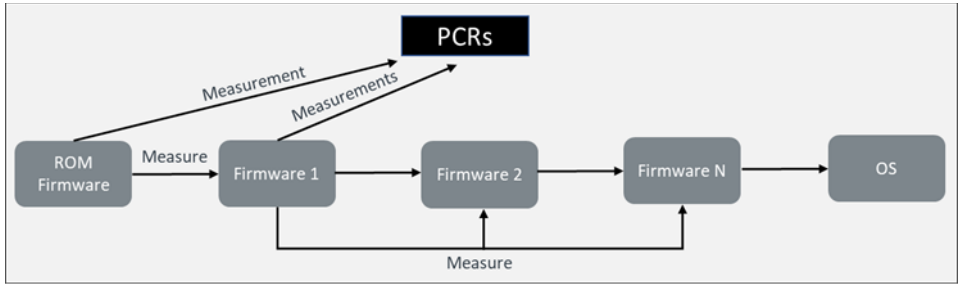
- **Be architecture agnostic (x86, Arm)**
- **Maintain the integrity of the platform layer and provide a safe execution environment for Akraino Blueprint software stacks**
- **Define secure boot requirements**
- **Attestation of the platform's secure state**
- **Protection of key assets in the platform (platform ID, encryption keys, configuration data, etc.)**
- **Secure platform firmware update**



Section One: Platform Security

- Verified (Secure) Boot
- Measured Boot
- Trusted Computing Base (TCB)
- Platform Root of Trust (RoT)
  - Immutable RoT
  - RoT for Measurement
  - RoT for Verification
  - Rot for Update
- Isolation of Trusted Processes
- Platform Boot Flows





Section Two: Questionnaire

- **Define use cases for the Akraino Platform Security Architecture questionnaire:**
  - **Blueprint creators**
  - **Blueprint users**
  - **Chip providers**
  - **Platform providers**
  - **Organizations**
- **Platform Security questionnaire**
- **System Software Security questionnaire**

AKRAINO

Section Three: Platform Security Implementations

- **Akraino PSA Whitepaper provides an overview of platform-specific implementation of security requirements from Arm and Intel:**
  - **Arm Platforms**
    - **Platform Boot Flow**
    - **Trusted Boot**
    - **Chain of Trust**
    - **Execution and Security States**
  - **Intel Platforms**
    - **Platform Boot Flow with Intel© Boot Guard and TPM**
    - **Measured Boot**
    - **Verified Boot**

- **Trusted Platform Module (TPM)**

Akraino PSA Whitepaper Publishing and Availability

- **Akraino PSA Whitepaper is complete and approved by the TSC for publishing.**
- **Publication status:**
  - **Publication in progress**
  - **LF Edge publications web page (https://www.lfedge.org/resources/publications)**
  - **Available in a few weeks**

Questions